Patentansprüche

1. Verfahren zur Datenübertragung mit folgenden Schritten:

- Eingabe von ersten Daten aus einem stochastischen Prozess (114) in zumindest erste und zweite Teilnehmer (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) eines Kommunikationsnetzes (100, 106; 400, 406; 500, 514, 518),

- in jedem der zumindest ersten und zweiten Teilnehmer: Erzeugung eines symmetrischen Schlüssels (S1, S2), basierend auf den ersten Daten und Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern,

dadurch gekennzeichnet,

dass jeder der zumindest ersten und zweiten Teilnehmer über Mittel (108; 408) für zumindest ein erstes und ein zweites Verschlüsselungsverfahren zur Schlüsselerzeugung verfügt, wobei basierend auf den ersten Daten jeweils erste bzw. zweite symmetrische Schlüssel erzeugt werden, und dass für die verschlüsselte Datenübertragung in zeitlicher Reihenfolge zwischen den ersten und zweiten Verschlüsselungsverfahren gewechselt wird.

2. Verfahren nach Anspruch 1, wobei zur Erzeugung der ersten und zweiten Schlüssel in jedem der zumindest ersten und zweiten Teilnehmer verschiedene erste Daten durch unterschiedliche Kombinatorik der stochastischen Daten gebildet werden.

3. Verfahren nach Anspruch 1 oder 2, wobei die ersten Daten über das Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) übertragen werden.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei die ersten Daten durch Erfassung von mindestens einem Messwert aus dem stochastischen Prozess (114) gewonnen werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei es sich bei dem stochastischen Prozess um einen zeitlich veränderlichen Parameter eines Automatisierungssystems (500) handelt.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die ersten Daten aus niedersignifikanten Bit-Positionen (LSB) eines oder mehrerer Messwerte gewonnen werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei jeder der zumindest ersten und zweiten Teilnehmer stochastische Daten erfasst, aus denen die ersten Daten gebildet werden.

8. Verfahren nach Anspruch 7, wobei die ersten Daten aus den stochastischen Daten durch eine vorgegebene Kombinatorik gebildet werden.

9. Verfahren nach Anspruch 7 oder 8, wobei die stochastischen Daten über das Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) übertragen werden.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Erzeugung des symmetrischen Schlüssels in den Teilnehmern auf Anforderung eines Master-Teilnehmers des Kommunikationsnetzes erfolgt.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Erzeugung des symmetrischen Schlüssels zu vorbestimmten Zeitpunkten oder nach vorbestimmten Zeitintervallen in den zumindest ersten und zweiten Teilnehmern erfolgt.

12. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Übertragung der ersten Daten oder der stochastischen Daten zu einem Zeitpunkt geringer Auslastung des Kommunikationsnetzes erfolgt.

13. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Übertragung der ersten Daten oder der stochastischen Daten mit einem asymmetrischen Verschlüsselungsverfahren erfolgt.

14. Computerprogrammprodukt, insbesondere digitales Speichermedium, mit Programmmitteln zur Durchführung der folgenden Schritte:

- Eingabe von ersten Daten aus einem stochastischen Prozess (114) in zumindest erste und zweite Teilnehmer (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) eines Kommunikationsnetzes (100, 106; 400, 406; 500, 514, 518),

- in jedem der zumindest ersten und zweiten Teilnehmer: Erzeugung eines symmetrischen Schlüssels (S1, S2), basierend auf den ersten Daten und Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern,

dadurch gekennzeichnet,

dass jeder der zumindest ersten und zweiten Teilnehmer über Mittel (108; 408) für zumindest ein erstes und ein zweites Verschlüsselungsverfahren zur Schlüsselerzeugung verfügt, wobei basierend auf den ersten Daten jeweils erste bzw. zweite symmetrische Schlüssel erzeugt werden, und dass für die verschlüsselte Datenübertragung in zeitlicher Reihenfolge zwischen den Verschlüsselungsverfahren gewechselt wird.

15. Computerprogrammprodukt nach Anspruch 14, wobei die ersten Daten durch Erfassung eines Messwerts aus dem stochastischen Prozess (114) gewonnen werden.

16. Computerprogrammprodukt nach Anspruch 14 oder 15, wobei die ersten Daten aus niedersignifikanten Bit-Positionen (LSB) eines oder mehrerer Messwerte gewonnen werden.

17. Kommunikationssystem mit zumindest ersten und zweiten Teilnehmern (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) und einem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) für eine Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern, und mit:

- Mitteln (112) zur Eingabe von ersten Daten aus einem stochastischen Prozess (114) in die zumindest ersten und zweiten Teilnehmer,

- in jedem der zumindest ersten und zweiten Teilnehmer: Mittel (108; 408) zur Erzeugung eines symmetrischen Schlüssels basierend auf den ersten Daten und Mittel (110; 426; 520, 522) zur Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern,

dadurch gekennzeichnet,

dass jeder der zumindest ersten und zweiten Teilnehmer über Mittel (108; 408) für zumindest ein erstes und ein zweites Verschlüsselungsverfahren zur Schlüsselerzeugung verfügt, wobei basierend auf den ersten Daten jeweils erste bzw. zweite symmetrische Schlüssel erzeugt werden, und dass für die verschlüsselte Datenübertragung in zeitlicher Reihenfolge zwischen den Verschlüsselungsverfahren gewechselt wird.

18. Kommunikationssystem nach Patentanspruch 17, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um ein öffentliches Netz handelt.

19. Kommunikationssystem nach Patentanspruch 17 oder 18, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um das Internet handelt und ein Teilnehmer als Master-Teilnehmer ausgebildet ist, um eine Schlüsselerzeugung in den anderen Teilnehmern durch Übertragung einer entsprechenden Anforderung über das Internet auszulösen.

20. Kommunikationssystem nach Anspruch 17 oder 18, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um ein Ethernet handelt.

21. Kommunikationssystem nach Anspruch 20, wobei einer der Teilnehmer als Master-Teilnehmer ausgebildet ist, um auf das Ethernet ein Kommando zur Auslösung der Schlüsselerzeugung in den Teilnehmern auszugeben.

22. Kommunikationssystem nach einem der vorhergehenden Ansprüche 17 bis 21, wobei es sich bei den zumindest ersten und zweiten Teilnehmern um Komponenten eines Automatisierungssystems (500) handelt.

23. Kommunikationssystem nach einem der vorhergehenden Ansprüche 17 bis 22, wobei zumindest einer der Teilnehmer (516) zur Durchführung einer Fernwartung ausgebildet ist.